Network Device Interpretation # 2021004

Elliptic curve-based key establishment and NIST SP 800-56Arev3

Status: ☒ *Active* ☐ *Inactive*

Date: *29-Mar-2021*

End of proposed Transition Period (to be updated after TR2TD process): *29-Apr-2021*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPPv2.2e*

Affected Section(s): *FCS_CKM.2*

Superseded Interpretation(s): *None*

Issue:

There is no appropriate selection in NDcPPv2.2e FCS_CKM.2 for TOE that implement NIST SP 800-56Arev3 conforming Elliptic curve-based key establishment scheme. This is especially problematic as claims of compliance to older versions of NIST SP 800-56A would result in CMVP certificate archival after December 31, 2021.

Standard validity timeline:

Standard	**Released**	**Withdrawn**	**NIST algorithm validation availability**
SP 800-56A	March 2006	March 14, 2007	Yes (though December 2021)
SP 800-56Arev1	March 2007	June 05, 2013	Never available
SP 800-56Arev2	May 2013	April 16, 2017	Never available
SP 800-56Arev3	April 2018		Yes (added October 2020)

The existing EC selection in FCS_CKM.2.1 explicitly references NIST Special Publication 800-56A Revision 2 and is therefore problematic to claim and support with a FIPS 140-2 certified module.

Please update FCS_CKM.2 selections with an option for TOE implementing certified elliptic curve-based key establishment scheme conforming to SP 800-56Arev3.

Resolution:

The selection for Elliptic curve-based key establishment in FCS_CKM.2.1 shall be modified as follows:

<add>

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*

</add>

shall be added as additional option in FCS_CKM.2.1.

Rationale:

See "Issue" section

Further Action:

None.

Action by Network iTC:

None.